

WHAT IS CLAIMED IS;

1 1. A device for verifying identity of an authorized user prior to providing information
2 permitting said user to obtain access to a secure site, said device comprising:
3 ✓ a) a portable body member;
4 ✓ b) input means mounted to said body member for receiving physical presentation of a
5 unique biometric parameter of an individual;
6 ✓ c) first circuit means mounted to said body member for generating a biometric template
7 uniquely associated with the biometric parameter presented to said input means;
8 ✓ d) second circuit means mounted to said body member for storing a single biometric
9 template commensurate with said biometric parameter of said authorized user;
10 ✓ e) third circuit means mounted to said body member for comparing other biometric
11 templates, generated in response to presentation of biometric parameters to said first input
12 means subsequent to storage of said single biometric template, with said single biometric
13 template;
14 f) fourth circuit means mounted to said body member for generating a unique electrical
15 signal in response to substantial identity of the biometric template of a subsequently presented
16 biometric parameter with said single biometric template;
17 g) fifth circuit means mounted to said body for storing a sequence of alphanumeric
18 characters representing a unique PIN enabling said user to gain access to said secure site; and
19 h) communicating means mounted to said body member for recalling said unique PIN
20 in response to generation of said unique electrical signal.

1 2. The device of claim 1 and further including a plurality of manually operable keys
2 mounted to said body member, at least one of said keys being operable to actuate said second
3 circuit means to store said single biometric template.

1 3. The device of claim 1 wherein said fifth circuit means comprise memory means for
2 storing a plurality of said PINs each associated with a respective one of said secure sites.

1 4. The device of claim 1 and further including means for randomly generating said
2 sequence of alphanumeric characters.

1 5. The device of claim 1 wherein said communicating means comprises means for
2 generating a visual display, mounted to said body, of said unique PIN.

1 6. The device of claim 1 wherein said communicating means comprises an output port
2 mounted to said body.

1 7. The device of claim 1 wherein said biometric parameter is a finger print.

1 8. In a personal authentication device having a hand-held body member containing
2 means for generating, storing and communicating one or more alphanumeric passwords
3 necessary to gain access to one or more respective secure sites, enabling means for activating
4 said generating, storing and communicating means, said enabling means comprising:

5 a) input means mounted to said body member for receiving physical presentations of
6 a predetermined biometric parameter of an individual;

7 b) first circuit means mounted to said body member for generating a biometric template
8 commensurate with each presentation of said biometric parameter;

9 c) storage means mounted to said body member for storing a single biometric template;

10 d) comparing means mounted to said body member for comparing biometric templates
11 of biometric parameters presented to said input means with said single biometric template; and

12 e) second circuit means mounted to said body member for providing access to said
13 passwords in response to substantial identity of a template of a biometric parameter presented
14 to said input means and said single biometric template.

1 9. The enabling means of claim 8 wherein second circuit means comprises a visual
2 display of said password.

1 10. The enabling means of claim 9 wherein said visual display is an LCD visible
2 through a window on said body member.

1 11. The enabling means of claim 8 wherein said circuit means comprises an output port
2 for accepting a connector to transmit electrical signals commensurate with said password to an
3 external computer.

1 12. The enabling means of claim 8 wherein said biometric parameter is a finger print
2 and said input means comprises a finger print presentation pad.

1 13. The enabling means of claim 12 and further comprising at least one key mounted
2 to said body member, said storage means being operable to store said single biometric template
3 in response to simultaneous presentation of said biometric parameter to said input means and
4 pressing said key.

1 14. The enabling means of claim 8 wherein said device provides access to any of a
2 plurality of passwords each associated with a respective secure site and further comprising
3 selecting means mounted to said body member for selecting which of said passwords access
4 is desired.

1 15. The enabling means of claim 14 wherein said selecting means comprise a plurality
2 of keys mounted to said body member.

1 16.. The method of verifying personal identity of an authorized user in possession of
2 a portable, stand-alone, electronic device and for providing information necessary to gain
3 access to a secure site in response to such verification, said method comprising:
4 a) physically presenting to said device a biometric parameter of said authorized user;
5 b) generating, by circuit means mounted to said device, a single biometric template
6 commensurate with said biometric parameter;
7 c) storing, by circuit means mounted to said device, said single biometric template;
8 d) comparing, by circuit means mounted to said device, biometric templates generated
9 in response to presentation of said biometric parameter subsequent to storage of said single
10 biometric template with said single biometric template;

11 e) generating, by circuit means mounted to said device, a unique electrical signal in
12 response to substantial identity of said compared biometric templates; and
13 f) providing said information in response to generation of said unique electrical signal.

1 17. The method of claim 16 and further comprising:

2 a) storing, by circuit means at said secure host, a predetermined sequence of electrical
3 signals representing a multi-character PIN required for access to said secure site; and

4 b) storing, by circuit means mounted to said device, said predetermined sequence of
5 electrical signals.

1 18. The method of claim 17 wherein said step of providing said information includes
2 displaying said PIN by display means mounted to said device and communicating said PIN to
3 said secure site.

1 19. The method of claim 18 wherein said PIN is communicated to said secure site by
2 entering, via a keyboard independent of said device the characters of said PIN.

1 20. The method of claim 19 wherein said keyboard is operatively connected to a PC
2 which may be selectively placed in communication with a computer associated with said
3 secure site.

ADD
A1

add
B1